Third-party suppliers play an ever-increasing role for all organizations. And as critical as these suppliers are, they can introduce significant risk if not monitored and managed effectively. In study after study, executives and board members want reports on the status of vendor risk—but if risk is managed by spreadsheets, how accurate are those reports?

Watch the warning signs

In a recent study about third party risk, 45% of the respondents had experienced a data breach and 55% had a compliance issue, both of which originated with a third party.

7 steps to a resilient, risk-based vendor management program

1. Digitize, consolidate, and integrate all aspects of vendor information and the vendor management lifecycle
2. Get granular into where risk originates with meaningful risk assessments that include subsidiaries—assess early and often
3. Generate cybersecurity scores to compare, prioritize, and communicate risk
4. Collaborate with vendors and keep an audit trail
5. Utilize machine learning and automation to reduce costs and do more with less
6. Build a resiliency plan and embed it into every aspect of your vendor management program
7. Integrate with third parties, such as BitSight for security ratings, for continuous monitoring and management of your risk posture

Access BitSight for Third Party Risk Management in the ServiceNow Store.

© 2020 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1 The 2020 Third-Party Risk Management Study by Prevalent and Shared Assessments
2 BitSight Easy Security Wins: How Patching and Software Updates Impact Your Cybersecurity